Encryption DataPort
User's Manual

Benutzerhandbuch

www.CRU-DataPort.com

CRU-DataPort wurde 1986 in Vancouver, Washington gegründet und hat dort seinen Hauptsitz. Das Unternehmen entwickelt und vertreibt Geräte zum Sichern und Speichern von Computerdaten. Die DataPort™-Produktreihe auswechselbarer Speichermodule, mit weltweit über 2 Millionen installierten Einheiten, gilt als Standard im Bereich der Datensicherheit. Behörden, Bildungsinstitute und IT-Abteilungen in Unternehmen wissen, dass sie diesen auswechselbaren Speichermodulen vertrauen können. DataPorts wurden für 25 000 Einschubvorgänge bewertet und enthalten Lüfter zum Schutz Ihrer Festplatte.

CRU-DataPort-Produkte sind weltweit bei führenden Distributoren, Original-Computerherstellern, zahlreichen Wiederverkäufern und Systemintegratoren und im Fachhandel erhältlich. Weitere Informationen über CRU-DataPort finden Sie auf unserer Website unter www.CRU-DataPort.com.

CRU-DataPort i

Allgemeine Beschreibung 1

Verschlüsselung 1
- DES (Data Encryption Standard) 1
- TDES (Triple DES) 1

Encryption DataPort-Features..... 1

Paketinhalt von DataPort V "Plus" Encryption..... 3

Vorbereitung der Installation..... 4

Rahmeninstallation 4

Festplatteninstallation 6

Betrieb 8
- Verwendung von Sicherheitsschlüsseln 8
- Schritte für den Betrieb 9

LED-Funktionen 10

Lüfterausfallalarm 10

Fehlerbehebung 11
Technischer Support 12

Beschränkte Garantie 12
- Produktansprüche 12
- Haftungsbeschränkung 12

Allgemeine Beschreibung

Das auswechselbare Speichermodul CRU-DataPort ermöglicht das leichte Herausnehmen einer 3,5-Zoll-Festplatte aus Ihrem PC, MAC, Ihrer Arbeitsstation oder Ihrem Festplattenarray-Subsystem.

Ein DataPort besteht aus einem Rahmen und Gehäuse mit Abdeckungen oben und unten. Der Rahmen passt in alle Standard-5,25 Zoll-Laufwerkseinschübe. DataPort-Modelle sind für Serial ATA-, IDE- und SCSI-Schnittstellen erhältlich und können mit einem Schloss oder Riegeln konfiguriert werden. Es sind auch Encryption DataPort-Modelle mit IDE-Schnittstelle mit Chiffrierschlüsseln in unterschiedlichen Stärken (40, 64, 128 und 192 Bit) erhältlich.

Verschlüsselung

DES (Data Encryption Standard)

Der Encryption DataPort V “Plus” verwendet zum Verschlüsseln der gesamten Festplatte den DES- oder TDES-Algorithmus. Ein DES-Algorithmus mit einem geheimen elektronischen 64-Bit-Schlüssel wird als Chiffrierschlüssel bezeichnet. DES verändert die ursprünglichen Daten mit einem geheimen elektronischen 64-Bit langen (oder länger) Schlüssel. Nach Anwendung der DES-Verschlüsselung spricht man von verschlüsseltem Text. Wird die DES-Verschlüsselung rückgängig gemacht, spricht man vom Entschlüsseln. Zum Wiederherstellen der ursprünglichen Daten ist beim Entschlüsseln ein korrekter (bitgenauer) geheimer elektronischer Schlüssel erforderlich. Bei der Verwendung des falschen Schlüssels zum Entschlüsseln ist das Ergebnis unlesbar.

TDES (Triple DES)

Triple DES (TDES) umfasst drei (3) nacheinander ausgeführte DES-Vorgänge. Beim ersten Durchgang verschlüsselt DES die Daten mit einem geheimen elektronischen Schlüssel (Schlüssel 1). Beim zweiten Durchgang wird das Ergebnis der ersten Verschlüsselung mit einem zweiten geheimen elektronischen Schlüssel (Schlüssel 2) verarbeitet. Beim dritten Durchgang wird das Ergebnis der zweiten Verschlüsselung mit einem dritten geheimen elektronischen Schlüssel (Schlüssel 3) verschlüsselt.

Encryption DataPort-Features

Wir gratulieren Ihnen zum Kauf eines CRU-DataPort Encryption DataPort V “Plus.” Sie verfügen jetzt über ein leistungsfähiges Zugriffssteuerungs-/Verschlüsselungssystem zum Schutz Ihrer Daten. Die bahnbrechende Technologie des Encryption DataPort V “Plus” bietet auf gleicher Ebene Schutz wie bei militärischen Einrichtungen.

Encryption DataPort V “Plus” ist mit einem Echtzeitprozessor ausgestattet, der den gesamten Festplatteninhalt – einschließlich Bootsektor, temporärer Dateien, Auslagerungsdateien und

Betriebssystem – Bit für Bit ohne Leistungsverlust verschlüsselt. Der Encryption DataPort V “Plus” ist für den Benutzer vollständig transparent. Der Benutzer benötigt weder Befehle noch eine grafische Benutzeroberfläche. Der Encryption DataPort V “Plus” ist extrem schnell und verarbeitet ohne zusätzliche CPU-Zeit und Systemressourcen 1,6 Gbit/s. Der Encryption DataPort V “Plus” ist mit allen Betriebssystemen kompatibel und erfordert keine Gerätetreiber.

Der Encryption DataPort V “Plus” verwendete eine NIST-Engine (National Institute of Standards and Technology) – eine zertifizierte 64-Bit-DES und 128/192-Bit-TDES-Hardware-Engine zur Echtzeitverschlüsselung und -entschlüsselung. Diese zertifizierten Algorithmen bieten zuverlässige Sicherheit. Werden sie in voller Stärke eingesetzt, ist es nahezu unmöglich, auf die verschlüsselten Daten durch Erraten oder Ableiten des richtigen TDES-Schlüssels zuzugreifen. Da der gesamte Festplatteninhalt verschlüsselt wird, sind Ihre Daten auch dann sicher, wenn Angreifer versuchen, von ihrer eigenen Festplatte zu booten oder Ihre Festplatte auf einen ungesicherten Computer zu verschieben.

Der Encryption DataPort V “Plus” ist mit den standardmäßigen DataPort V & V “Plus”-Rahmen (IDE-Version) kompatibel. Da die Hardwareverschlüsselungs-Engine im Gehäuse enthalten ist, kann mit bereits installierten DataPort V- und V “Plus”-Rahmen ein Gehäuse mit einem verschlüsselten Laufwerk verwendet werden. Das Gehäuse und der zum Verschlüsseln der Festplatte verwendete Sicherheitsschlüssel (der Schlüssel mit dem geheimen elektronischen Code) können in mehreren DataPort V- oder V “Plus”-Rahmen verwendet werden. Daher kann das Gehäuse mit der verschlüsselten Festplatte sicher in mehreren PCs verwendet werden. Mehrere Benutzer, die alle ein eigenes Encryption DataPort V “Plus”-Gehäuse mit einem eindeutigen Sicherheitsschlüssel besitzen, können denselben PC auf sichere Weise verwenden. Mit dem Encryption DataPort V “Plus” können Sie Ihre Daten verschlüsseln, ohne auf die mit DataPort ermöglichte Mobilität und Sicherheit zu verzichten.

Paketinhalt von DataPort V “Plus” Encryption

Das DataPort-Paket enthält alle Hardwarekomponenten, die zur Installation eines 3,5-Zoll-Laufwerks in einen 5,25-Zoll-Laufwerkseinschub erforderlich sind. Überprüfen Sie vor der Installation, ob der folgende Paketinhalt vorliegt.

Menge	Beschreibung
1	DataPort V “Plus”-Rahmen
1	DataPort V “Plus”-Gehäuse
2	Metallabdeckungen
4	6-32 x 3/8-Zoll-Senkschrauben zur Befestigung der Festplatte
4	M3 x 10-mm-Kreuzschlitzschrauben zur Befestigung des Rahmens
2	Sicherheitsschlüssel für die Verschlüsselung (zwei Schlüssel)
2	Schlüssel für Sperrschloss

Fehlt eine der oben genannten Komponenten, oder benötigen Sie spezielle Teile, wenden Sie sich an Ihren Fachhändler oder an CRU-DataPort. Sie können weitere Encryption DataPort-Gehäuse oder Rahmen für mehrere Laufwerke bestellen.

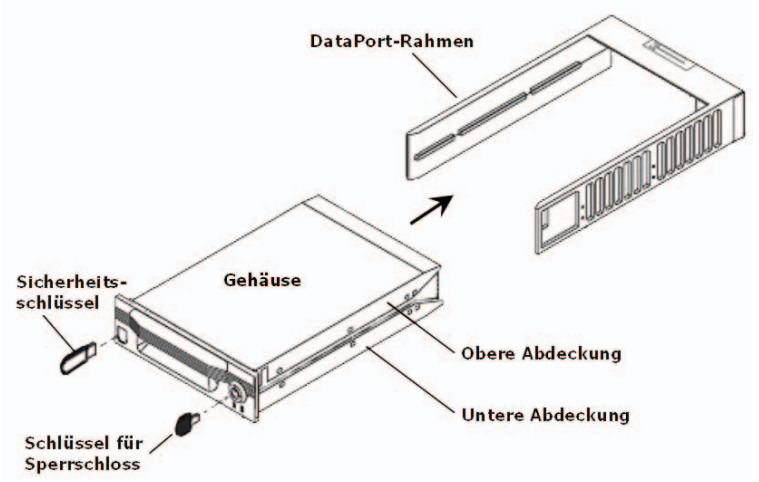

Abbildung 1 – Verwendung des Paketinhaltes

Vorbereitung der Installation

1. Lesen Sie dieses Handbuch genau durch, bevor Sie den DataPort installieren oder verwenden, um den Verlust von Daten zu vermeiden.

2. Stellen Sie vor dem Berühren elektrischer Geräte eine Erdung her, indem Sie ein Metallteil des Computergehäuses berühren. Durch diese elektrostatische Entladung können Sie einer Beschädigung des Computers vorbeugen. CRU-DataPort ist nicht verantwortlich für Schäden, die durch elektrostatische Entladung entstehen.

3. Sie benötigen folgende Werkzeuge und Gegenstände:

   - Kreuzschlitzschraubenzieher
   - Kleiner flacher Schraubenzieher
   - Benutzerhandbuch des Computers
   - Festplattenhandbuch zum Konfigurieren des Master-Jumpers

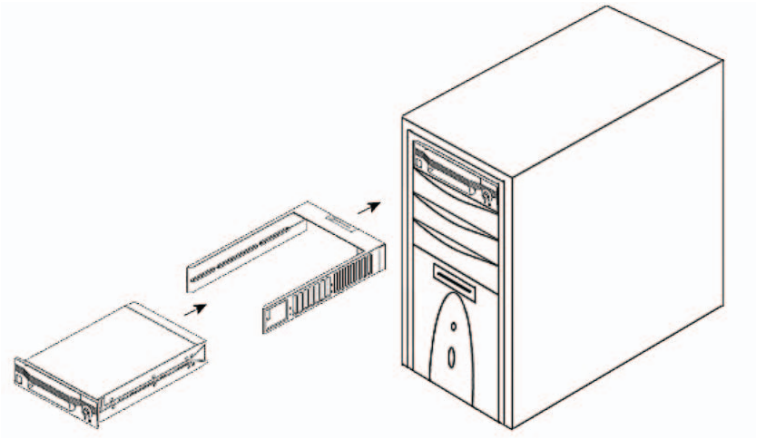

Abbildung 2 – Einbau

Rahmeninstallation

1. Schalten Sie den Computer aus, und ziehen Sie das Stromkabel aus der Steckdose. Warten Sie vor dem Arbeiten am Computer eine Minute, bis der Reststrom abgeleitet wurde.

2 Entfernen Sie die Abdeckung vom Computer.

3. Suchen Sie nach einem extern zugänglichen 5,25-Zoll-Laufwerkseinschub.

4. Sind für den Laufwerkseinschub Befestigungsschienen erforderlich, montieren Sie diese am Rahmen. Die Befestigungsschienen sind im Lieferumfang Ihres Computers enthalten.

5. Schieben Sie den Rahmen in den 5,25-Zoll-Einschub. Befestigen Sie den Rahmen mit den mitgelieferten Schrauben.

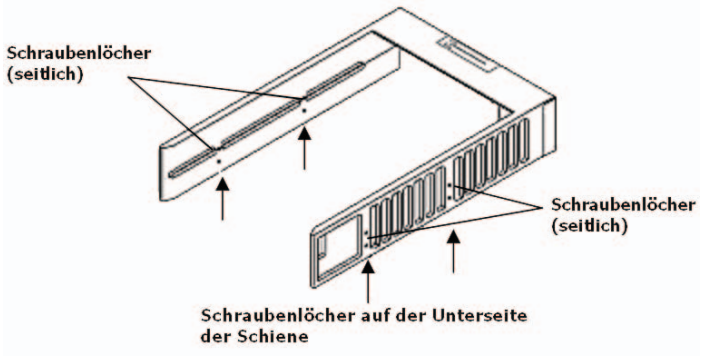

Abbildung 3 – Position der Schraubenlöcher

6. Schließen Sie ein Gleichstromkabel am Rahmen an. Schließen Sie ein freies vierpoliges Gleichstromkabel des Computernetzteils an der Buchse am Rahmen an (siehe Abbildung 4).

7. Schließen Sie das Datenkabel am Rahmen an.

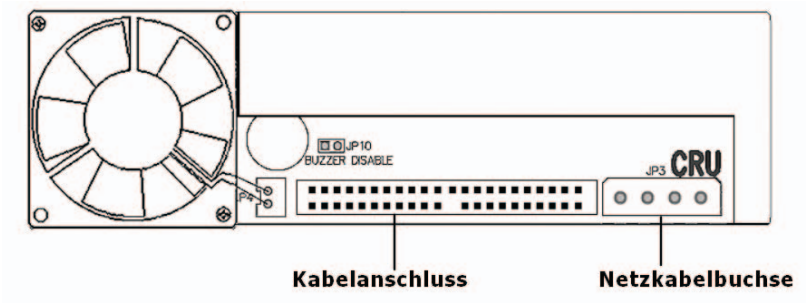

Abbildung 4 – DataPort-Rückansicht

Die Rahmeninstallation ist somit abgeschlossen.

Festplatteninstallation

WICHTIG! Lesen Sie diese Informationen vor der Installation.

Lesen Sie die folgenden Abschnitte vor dem Einrichten Ihres Encryption DataPort V “Plus”, um Datenverlust vorzubeugen.

Warnhinweis! Sichern Sie Ihre Daten vor jeder Hardwareinstallation.

Die Einrichtung des Encryption DataPort V “Plus” setzt die Formatierung Ihrer Festplatte voraus. Beim Formatieren gehen alle Daten auf Ihrer Festplatte verloren. Da Sie Ihre Festplatte formatieren, müssen Sie alle Daten, die Sie behalten möchten, sichern. Sichern Sie die Daten vor dem Installieren des Festplattenlaufwerks im DataPort.

1. Entfernen Sie die obere und untere Gehäuseabdeckung. Verwenden Sie hierzu das mitgelieferte Werkzeug zum Entfernen der Abdeckung oder einen kleinen flachen Schraubenzieher.

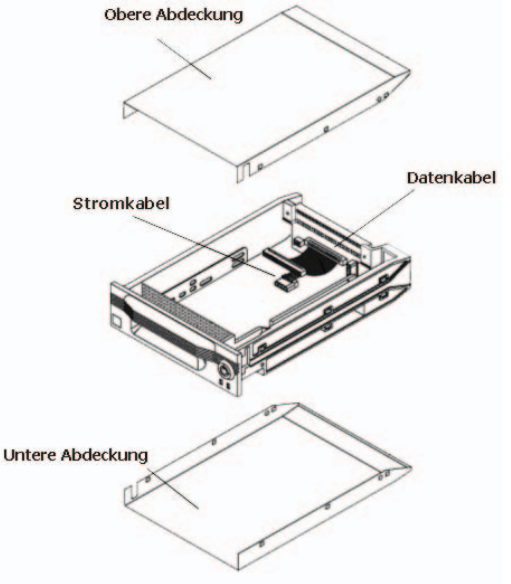

Abbildung 5 – Innenansicht des Gehäuses

2. Stellen Sie den Master/Slave-Jumper des Laufwerks ein, bevor Sie das Laufwerk im Gehäuse platzieren. Schlagen Sie im Benutzerhandbuch zu Ihrer Festplatte nach, wie die Festplatte mittels Jumper als Master oder Slave konfiguriert wird. Vergewissern Sie sich vor dem Einschieben des Laufwerks, dass auch der Jumper des Gehäuses korrekt eingestellt ist.

3. Stellen Sie die Jumper des Encryption DataPort V “Plus”-Gehäuses ein.

   Zur Auswahl stehen drei Jumperpositionen. Der Encryption DataPort V “Plus” ist für Masterlaufwerke vorkonfiguriert. Abbildung 6 enthält alternative Konfigurationen für Ihr Laufwerk.

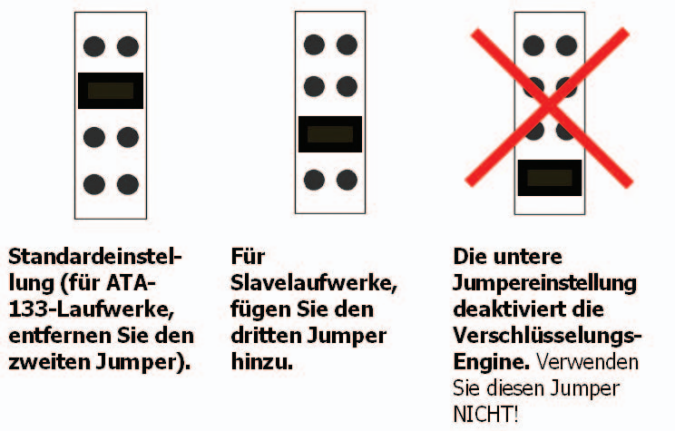
Standardeinstel-lung (für ATA-133-Laufwerke, entfernen Sie den zweiten Jumper).
Für Slavelaufwerke, fügen Sie den dritten Jumper hinzu.
Die untere Jumpereinstellung deaktiviert die Verschlüsselungs-Engine. Verwenden Sie diesen Jumper NICHT!

Abbildung 6 – Jumperpositionen

   Hinweis: Der untere Jumper ist für spezielle von CRU-DataPort durchgeführte Tests vorgesehen. Bei Verwendung dieses Jumpers wird die Verschlüsselung Ihrer Daten verhindert.

4. Schließen Sie das Gleichstromkabel am Laufwerk an: Stecken Sie das vierpolige Gleichstromkabel am Stromanschluss des Laufwerks an, und vergewissern Sie sich, dass es fest sitzt.

5. Schließen Sie das Datenkabel am Laufwerk an.

6. Installieren Sie das Laufwerk: Platzieren Sie das Laufwerk im Gehäuse, und befestigen Sie es mit den vier mitgelieferten Schrauben. Platzieren Sie die Kabel im Gehäuse, so dass diese vollständig darin verstaut sind.

7. Befestigen Sie den Temperatursensor (TCCS) mit Klebeband oben auf der Festplatte.

8. Bringen Sie die obere und untere Abdeckung wieder an, nachdem Sie alle Kabelverbindungen überprüft haben.

Betrieb

Die für den Betrieb erforderlichen Schritte folgen der Beschreibung der Verwendung von Sicherheitsschlüsseln. Lesen Sie den Abschnitt über Sicherheitsschlüssel vor der Verwendung der Festplatte.

Verwendung von Sicherheitsschlüsseln

Der Encryption DataPort V “Plus” wird mit Sicherheitsschlüsseln geliefert, die Sie als autorisierten Benutzer authentifizieren und die Verschlüsselung/Entschlüsselung ermöglichen. Ohne den mitgelieferten Sicherheitsschlüssel kann Ihr Computer NICHT gestartet werden, und/oder die Daten auf der Festplatte sind NICHT einsehbar. Testen Sie den zweiten Schlüssel, nachdem Sie den Encryption DataPort eingerichtet haben, um sicherzustellen, dass dieser korrekt funktioniert.

WICHTIG!

Stecken Sie den Sicherheitsschlüssel niemals in einen FireWire-Port!! Der Sicherheitsschlüssel wird beschädigt, wenn Sie ihn in einen FireWire-Port stecken. Der Schlüssel ist dann nicht mehr verwendbar, was zu einem Datenverlust führen kann.

Bewahren Sie den zweiten Sicherheitsschlüssel immer an einem sicheren Ort auf!!

Der Sicherheitsschlüssel enthält den geheimen elektronischen Schlüssel für die DES/TDES-Echtzeit-Schlüssel-Engine. Ohne diesen eindeutigen geheimen elektronischen Schlüssel ist der Zugriff auf die Daten auf der verschlüsselten Festplatte nicht möglich. Bewahren Sie den Zweitschlüssel an einem sicheren Ort auf, falls Sie den Originalschlüssel verlieren.

Beim Verlust beider Sicherheitsschlüssel können Ihre Daten nicht wiederhergestellt werden.

Der Encryption DataPort V “Plus” besitzt keine „Hintertür“. CRU-DataPort verfügt über keine Unterlagen über den auf dem Sicherheitsschlüssel gespeicherten geheimen elektronischen Schlüssel und kann keinen Ersatz anbieten. CRU-DataPort bietet jedoch einen Duplizierungsdienst. Voraussetzung hierfür ist die Einsendung des Originalschlüssels an CRU-DataPort.

Alle Encryption DataPort V “Plus”-Einheiten werden vor der Lieferung ausführlich getestet und erfüllen die hohen Qualitätsstandards, die Sie von CRU-DataPort gewohnt sind. Sollte ein Encryption DataPort V “Plus” trotz allem nicht funktionieren, geben Sie das Gehäuse an CRU-DataPort zurück. Solange Sie den Originalsicherheitsschlüssel besitzen, sind die Daten auf der Festplatte nicht verloren.

1. Stecken Sie den Sicherheitsschlüssel in den Schlüsselport auf der Vorderseite des Encryption DataPort V “Plus”. Der Sicherheitsschlüssel muss vor dem Einschalten des Encryption DataPort V “Plus” eingesteckt werden.

   Ohne den korrekten Sicherheitsschlüssel kann Ihr Computer NICHT gestartet werden, und/oder die Daten auf der Festplatte sind NICHT einsehbar.

2. Entfernen Sie den Sicherheitsschlüssel nach dem Starten des Computers, und bewahren Sie ihn an einem sicheren Ort auf. Durch das Entfernen des Sicherheitsschlüssels nach dem Start des Computers wird der Computerbetrieb nicht beeinflusst.

Hinweis: Der Schlüsselport auf der Vorderseite des DataPort-Gehäuses ist nur für den Sicherheitsschlüssel bestimmt. Dieser Schlüsselport ist mit dem IEEE-1394-FireWire-Anschluss aus mechanischer Sicht identisch, jedoch ist diese Schlüsselbuchse keine FireWire-Schnittstelle. Schließen Sie am Sicherheitsschlüsselport keine FireWire-Produkte an.

3. Schalten Sie den DataPort ein.

   Das Sperrschloss des DataPort befestigt das Gehäuse und dient auch zum Ein-/Ausschalten. Drehen Sie Sperrschloss um 90 Grad im Uhrzeigersinn in die Stellung ON, bevor Sie den Computer einschalten.

4. Jetzt müssen Sie die Festplatte FORMATIEREN. Durch das Formatieren werden die Festplatte auf die Verwendung vorbereitet und der Bootsektor und die Dateizuordnungstabelle (File Allocation Table – FAT) verschlüsselt.

WARNHINWEIS!

Beim FORMATIEREN wird der gesamte Festplatteninhalt gelöscht. Sichern Sie Ihre Daten vor diesem Vorgang. Wir übernehmen keine Verantwortung für verlorene Daten.

Beim Formatieren Ihrer Festplatte werden alle Daten gelöscht. Sichern Sie also vor dem Formatieren alle Daten auf dem Laufwerk. Der Encryption DataPort V “Plus” erfordert die Formatierung der Festplatte, unabhängig davon, ob das Laufwerk neu oder alt ist. Führen Sie den Standardbefehl FDISK oder FORMAT Ihres Betriebssystems aus. Laden Sie nach dem Formatieren die Betriebssystemdateien und alle anderen benötigten Dateien einschließlich aller gesicherten Dateien. (Wenden Sie sich an den technischen Support von CRU-DataPort, wenn Sie für diesen Schritt technische Unterstützung benötigen.)

Hiermit ist die Installation abgeschlossen, und das DataPort-Laufwerk ist betriebsbereit.

LED-Funktionen

Die grüne LED und die Netzanzeige leuchten im eingeschalteten Zustand des DataPort. Die rote LED erfüllt zwei Funktionen. Leuchtet die rote LED während des Bootvorgangs ununterbrochen auf, besteht ein Problem mit dem Sicherheitsschlüssel. Der Sicherheitsschlüssel kann nicht gelesen werden und somit keine Daten ver- und entschlüsseln. Nach dem Booten fungiert die rote LED als Anzeige von Festplattenaktivität.

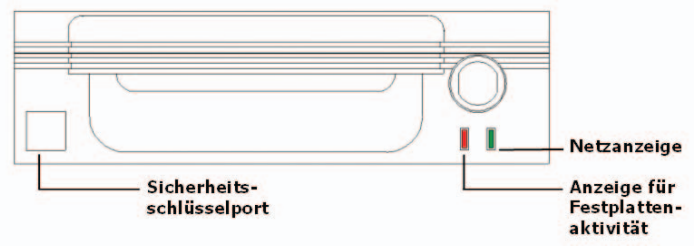

Abbildung 7 – DataPort-Vorderansicht

Lüfterausfallalarm

Der Lüfterausfallalarm ist eine Standardfunktion des DataPort V “Plus”. Bei einem Ausfall des Lüfters ertönt ein Alarmsignal, und die grüne LED unten rechts im DataPort-LED-Fenster leuchtet auf.

WICHTIG!

Lesen Sie die folgenden Informationen, bevor Sie das Gehäuse entfernen.

Das Entfernen des DataPort-Gehäuses bei laufendem Computer wird nicht empfohlen. Wenn Sie das Gehäuse bei laufendem Computer entfernen müssen, beachten Sie Folgendes:

- Warten Sie, bis die rote Anzeige für die Festplattenaktivität erlischt, wodurch signalisiert wird, dass keine Lese-/Schreibvorgänge ausgeführt werden.
- Vergewissern Sie sich bei der Verwendung eines Festplattencacheprogramms, dass alle Daten auf die Festplatte geschrieben wurden.

  Schalten Sie das Laufwerk aus, indem Sie den Schlüssel in die vertikale Position (OFF) drehen. Die grüne Anzeige erlischt, wodurch signalisiert wird, dass die Stromzufuhr unterbrochen ist. Warten Sie 10 bis 15 Sekunden, bis sich das Laufwerk nicht mehr dreht, und entfernen Sie anschließend das Gehäuse.

CRU-DataPort haftet nicht für den Verlust von Daten. Die Befolgung dieser wichtigen Richtlinien liegt in der Verantwortung des Benutzers.

Fehlerbehebung

Problem...	Lösung...
Keine Stromzufuhr	· Vergewissern Sie sich, dass sich das DataPort-Sperrschloss in der Position (ON) befindet und die grüne Anzeige leuchtet. · Überprüfen Sie die Verbindung des vierpoligen Gleichstromkabels im Gehäuse und auf der Rahmenrückseite.
Sicherheitsschlüsselfehler	· Die rote LED erfüllt zwei Funktionen. Leuchtet die rote LED während des Bootvorgangs ununterbrochen auf, besteht ein Problem mit dem Sicherheitsschlüssel. Der Sicherheitsschlüssel kann nicht gelesen werden und somit keine Daten ver- und entschlüsseln. · Vergewissern Sie sich, dass der Sicherheitsschlüssel im Schlüsselport steckt. Ist der korrekte Sicherheitsschlüssel nicht vorschriftsmäßig angeschlossen, wird das Laufwerk nicht gebootet oder nicht angezeigt.
Laufwerk wird vom Computer nicht erkannt.	· Überprüfen Sie zuerst alle Kabelverbindungen und die Jumperkonfiguration. · Überprüfen Sie die Master/Slave-Einstellung des Laufwerks. · Vergewissern Sie sich, dass das Gehäuse und der Rahmen fest sitzen, und beim Einschieben des Gehäuses keine Pins verbogen wurden. · Überprüfen Sie, ob ein Sicherheitsschlüsselfehler vorliegt. · Vergewissern Sie sich bei der Verwendung mehrerer Encrypted DataPorts, dass jeweils der korrekte Sicherheitsschlüssel verwendet wird.
Lüfterversagen	· Wenden Sie sich bei einem Lüfterversagen unter +1 (800) 260-9800 an den technischen Support von CRU-DataPort.

Technischer Support

Wenden Sie sich zuerst an den Fachhändler, wenn Sie technische Unterstützung benötigen. Benötigen Sie weitere technische Unterstützung, wenden Sie sich an den technischen Support von CRU-DataPort. Sie erreichen den technischen Kundendienst von CRU-DataPort über unsere Website unter http://www.CRU-DataPort.com oder per E-Mail an support@CRU-DataPort.com.

Beschränkte Garantie

CRU-DataPort gewährleistet während des Zeitraums von drei (3) Jahren nach dem ursprünglichen Kaufdatum, dass Encryption DataPort V “Plus” keine wesentlichen Material- und Verarbeitungsfehler aufweist.

Produktansprüche

Die gesamte Haftung von CRU-DataPort und der alleinige Anspruch des ursprünglichen Käufers besteht im Falle eines Gewährleistungsbruchs nach freiem Ermessen von CRU-DataPort (a) in der Erstattung des bezahlten Preises oder (b) in der Reparatur oder im Ersatz der Hardware – vorausgesetzt, die Hardware wird an CRU-DataPort mit einer Kopie des Kaufbelegs oder entsprechender Dokumentation zurückgegeben. Für jedes Hardwareersatzprodukt wird eine Garantie für die verbleibende Zeit der ursprünglichen Gewährleistungsdauer gewährt.

Diese Ansprüche entfallen, wenn der Ausfall der Hardware auf einen Unfall, einen Missbrauch, falsche Anwendung oder eine Änderung zurückzuführen ist (dies wird von CRU-DataPort festgelegt).

Haftungsbeschränkung

Die in dieser Vereinbarung festgelegten Garantien ersetzen alle anderen Garantien. CRU-DataPort lehnt ausdrücklich alle anderen Garantien ab, einschließlich, aber nicht beschränkt auf einschließlich, aber nicht beschränkt auf konkludente Garantien der Handelsüblichkeit und Eignung für einen bestimmten Zweck und Nichtverletzung von Rechten Dritter in Bezug auf die Dokumentation und Hardware. Kein CRU-DataPort-Händler,-Agent oder -Mitarbeiter ist berechtigt, diese Garantie zu ändern, verlängern oder zu erweitern.

CRU-DataPort oder seine Zulieferer haften unter keinen Umständen für Kosten, die für die Beschaffung von Ersatzprodukten oder-services entstehen, entgangenen Gewinn, Informations- oder Datenverlust, Computerausfall oder irgendwelche anderen speziellen, indirekten oder zufälligen Schäden oder Folgeschäden, die aufgrund des Verkaufs, der Verwendung oder der nicht möglichen Verwendung eines CRU-DataPort-Produkts oder -Services entstehen, und zwar auch dann, wenn CRU-DataPort über die Möglichkeit solcher Schäden informiert wurde. In keinem Fall darf die Haftbarkeit von CRU-DataPort den tatsächlich für die betroffenen Produkte bezahlten Geldbetrag übersteigen.